The consequences of the *Schrems* case and eHealth

Should medical doctors, clinical trial researchers, or information scientists in biotech or health information management lose any sleep over a case brought against Facebook? Griet Verhenneman, of the KU Leuven Centre for IT & IP Law, believes they should. What started as a request by Austrian Maximillian Schrems to investigate data transfers from Facebook Ireland Ltd. to Facebook Inc., turned into a landmark judgment by the European Court of Justice ('CJEU') on international data transfers, with far-reaching consequences. The CJEU has declared the US Adequacy Decision, generally cited as the Safe Harbor Decision ('Decision'), null and void. Consequently some 4,000 US companies, who transfer data between the EU and the US based on the Decision need to review their data transfers, as Griet explains.

In summer 2013 Max Schrems filed a complaint with the Irish Data Protection Authority ('DPA') about Facebook Ireland Ltd., requesting an audit of the data Facebook was passing to the US National Security Agency ('NSA') following the Snowden revelations. The Snowden revelations showed that Facebook Inc. participated voluntarily in the US PRISM programme, potentially transferring personal data on EU citizens. But, the Irish DPA dismissed Schrems' request, arguing that national DPAs had no authority to investigate international transfers that took place under a Commission Adequacy Decision such as the 2000/520/EC decision.

Upon the dismissal of his application, Max Schrems took the case to the High Court in Dublin. The Irish High Court decided to request a preliminary ruling from the CJEU questioning the competence of national DPAs to investigate data transfers under Commission Adequacy Decisions. In its request for a preliminary ruling the Irish High Court indicated that following the Snowden revelations significant questions were raised as to the actual ability of the US to ensure an adequate level of protection and satisfy the requirements of articles 7 and 8 of the EU Charter of Fundamental Rights.

Following this request the CJEU first examined the distribution of competences between national DPAs and the EU Commission ('EC') on Adequacy Decisions taken on the basis of Article 25 of the 95/46/EC Data Protection Directive ('DPD'). The court ruled that such Adequacy Decisions are binding on EU Member States and can only be declared invalid by the CJEU. Nevertheless national DPAs do retain their full investigative powers. Moreover, they have an obligation to assess claims brought before them. In other words: a national DPA may not withdraw itself from its obligation to investigate claims by individuals by stating that the EC has already made a binding adequacy decision. This is in line with previous rulings of the CJEU stressing the function of DPAs as guardians of the fundamental right to data protection.

Secondly, the CJEU examined the validity of the Decision. First it annuled Article 1 of the Decision, stating that on the basis of the Decision the EC cannot ensure an adequate level of protection through domestic law or international commitments. Secondly the court also annulled Article 3, which limited the powers of investigation of national DPAs. The court found that such a restriction exceeds the EC's competences.

With two of its main articles declared invalid, the Decision is in practice null and void. And consequently the *Schrems* case resulted in a judgment with implications extending far beyond its original context as it extends to all data transfers between the EU and the US, including transfers in the eHealth context. The storage of electronic health records, the use of telemedicine solutions, cooperation in clinical trials, the deployment of wellness apps and health trackers of all kinds - if they involve the processing of personal data under EU law, they are potentially affected by the CJEU's judgment.

The Safe Harbor Decision: unique in its kind

During the same period that Max Schrems filed his complaint with the Irish DPA, the EC tried but failed at finding a political solution to the pressure the Snowden revelations put on the Decision. Viviane Reding, then EC Vice President, called for a review of the Decision by the end of 2013. She acknowledged that the Decision "may not be so safe after all." The weakest points of the Decision were listed as a) transparency, b) the limited options for EU citizens to enforce their rights and c) the lack of monitoring of companies operating under Safe Harbor, as the agreement was based on self-certification.

In this sense the Decision had always been an Adequacy Decision unique in its kind. The US has no classical data protection laws, but has instead a hybrid system combining constitutional rights against governmental intrusion

and a scattered set of specific laws on the use of commercial information. In itself the US legal framework was not considered equivalent to European standards, but the EC agreed that when US companies commit to the Decision, they operate under a framework which provides an adequate level of protection. The Decision thus differs from other adequacy decisions in the sense that it is a framework additional to the legal framework offered by domestic laws and international commitments, and in the sense that this framework is based on self-certification.

Safe Harbor 2.0

Julie Brill, Federal Trade Commissioner ('FTC'), reflected on these differences in her speech at the Amsterdam Privacy Conference. "The FTC with its many years of experience and nearly 100 privacy and security enforcement actions - not counting [the] 40 actions involving safe harbor issues - has been a highly important and highly expert force," she said. But, "The [CJEU] decision crystallizes what has been clear - or should have been clear - for a long time about privacy in Europe: it is a fundamental right that Europeans and their Court take very seriously." Looking out to the future, she continued by stating that: "we should create a new data transfer mechanism that strengthens the privacy protections that were in the Safe Harbor principles" and that everyone understands "the need to ensure that these substantive protections are more robust."

The message of Commissioner Brill aligns with the message that European Commissioner Vera Jourova sent in the aftermath of the Data Protection and Privacy Commissioners meeting in Amsterdam, which followed the Amsterdam Privacy Conference. Jourova indicated that the new framework that is being discussed by the EU and the US would a) include stronger oversight by the US Department of Commerce to ensure that companies comply, b) establish free of charge redress mechanisms, c) bring consumers more transparency about the way companies handle consumer data, and d) include strict rules on the further transfer of data to additional parties. "This will transform the system from a purely self-regulating one to an oversight system that is more responsive as well as proactive and backed up by significant enforcement, including sanctions," Jourova said.

The storage of EHRs, the use of telemedicine solutions, cooperation in clinical trials, the deployment of wellness apps and health trackers - if they involve the processing of personal data under EU law, they are potentially affected by the CJEU judgment

When comparing Jourova's 2015 statements to Reding's statements, they are not all that different. This raises the question as to whether the CJEU's decision to declare all transfers under the Decision unlawful can put enough pressure on the negotiations to finally make progress. Clearly the CJEU's annullment of the Decision does create an urge for advancements in the discussions, but at the same time, a fall back mechanism is still available - at least for now.

Article 26 DPD: a solution to circumvent the judgment?

The 'default' rule available for transfers to the US may have been annulled, but Article 26 (1) and 26 (2) DPD do still offer the opportunity to transfer personal data to the US.

Article 26 (1) provides an exhaustive list of exemptions from the central prohibition to transfer data to third countries without an adequate level of protection. Assuming that there is no discussion on the original legal basis for the processing of health data, data can subsequently be transferred to the US for example when:

- The data subject has given his/her unambiguous consent thereto;
- or the transfer is necessary in order to protect the vital interests of the data subject.

All of the exceptions under Article 26 (1) need to be interpreted restrictively. With regard to transfers to protect the vital interests of the data subject, this means its use should be limited to life-or-death situations.

Obtaining unambiguous informed consent from data subjects could be an option for example in clinical trials. Unambiguous consent to transfer the data to the US can be obtained at the time written consent is obtained for participation in the clinical trial. Also with regard to the use of mHealth apps, informed consent can fairly easily be obtained from the data subject at the time of registration. This is of course on the condition that the notification to the data subject about the data transfer is not hidden in some small print general conditions. Such informed consent could hardly be called 'unambiguous.' Additionally it must be noted that informed consent in the context of data transfers should be freely given. It is questionable if informed consent can still be considered freely given if the customer has no other option but to agree with the transfer of his/her data. But not in all eHealth scenarios is informed consent such a valid option. Informed consent is for example troublesome in cases of processing biomedical samples or genetic or genomic information, first of all because these types of data concern not just one data subject, but also potentially other persons. Secondly, the use of biomedical samples for research is often linked to broad or blanket consent, two concepts that are still contested

under European data protection law. Obtaining informed consent is also probably not so obvious when healthcare professionals or healthcare institutions wish to engage with US companies offering cloud-based storage and computation solutions. In such a case it would be highly impractical to have to obtain informed consent from every single patient before transferring their data.

With regard to the latter problem, it is however worth considering the solution offered by Article 26 (2) of the DPD, under which personal data can also be transferred to third countries when an adequate level of protection is reached through the use of appropriate contractual clauses or binding corporate rules. Appropriate contractual clauses are a set of clauses specifically regulating the data transfer between the data controller and data processor. They can consist of the standard contractual clauses as pre-approved by the EC or of *ad hoc* clauses approved by a national DPA. Binding corporate rules are legally binding data processing rules adopted by a company or a group of companies to create a safe haven for data transfers within a corporate group.

However, it seems many or all of the mechanisms under Article 26 are hanging by a thread. The CJEU not only indicated that the EC misjudged the Decision, but it also emphasised the powers of national DPAs to independently review, and potentially suspend or sanction, international data transfers. The Article 29 Working Party ('WP29') and the German DPA have already sent a clear message following up on this responsibility. They will not tolerate data transfers to third countries where there is no broad analysis of the third country's domestic laws and international commitments. Such transfers will not be tolerated under an Adequacy Decision, but neither will they be tolerated under the other instruments foreseen by the DPD such as those of Article 26.

The WP29 set the deadline for reaching an agreement with US authorities as the end of January 2016, but German DPAs announced they will immediately begin investigating data transfers to the US and will not be granting new approvals. The WP29 stressed that "businesses should reflect on the eventual risks they take when transferring data and should consider putting in place any legal and technical solutions in a timely manner to mitigate those risks and respect the EU data protection *acquis*." Hamburg's Data Protection Commissioner Johannes Caspar had even stronger words: "Anyone who wants to remain untouched by the legal and political implications of the judgement, should in the future consider storing personal data only on servers within the European Union."

Conclusion

Since actors in the eHealth domain are dealing with sensitive information, the call for businesses to reflect on the risks of transferring data should be taken seriously. National legislations and attitudes with regard to the processing of health data differ between EU Member States, but in most Member States healthcare professionals do have a natural sense of circumspection linked to the Hippocratic Oath. As a result cloud-based solutions for the storage of healthcare records for example have only recently begun to see adoption. More than in other sectors, contracts on cloud-based storage and computation already stipulate that data are not to leave the EU. But in many other healthcare sectors such as medical research, where openness is the key to advancement, the contrary will be true and restricting data transfers to the EU only would probably not be beneficial for mankind.

Griet Verhenneman Legal Researcher
KU Leuven Centre for IT & IP Law - iMinds, Belgium
griet.verhenneman@law.kuleuven.be

References:

- CJEU Case C-362-14 Maximillian Schrems v. Data Protection Commissioner.
- EC Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce.
- 95/46/EC Directive of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data.
- WP29 Statement on the implementation of the judgement of the CJEU of 6 October 2015 in the Maximilian Scherms v. Data Protection Commissioner case (C-362-14), Brussels, 16 October 2015.
- COM/2013/0847 final from the EC to the European Parliament and the council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU.
- C. Kuner, 'Extraterritoriality and regulation of international data transfers in EU data protection law,' International Data Privacy Law, 2015.
- Datenschutz Hamburg, 'Position paper of the data protection authorities to Safe Harbour,' 26 October 2015, www.datenschutz-hamburg.de
- F. Coudert, 'Schrems vs. Data Protection Commissioner: a slap on the wrist for the Commission and new powers for data protection authorities,' European Law Blog, 15 October 2015.
- G. Moody, 'Germany to investigate Google, Facebook over data transfers,' Law & Disorder/Civilization & Discontents, 27 October 2015.
- J. Brill, 'Transatlantic Privacy After Schrems: Time for An Honest Conversation,' Keynote Address at the Amsterdam Privacy Conference, 23 October 2015.
- N. Drozdiak, 'EU, US Agree in Principle on New Data-Transfer Pact,' The Wall Street Journal, 26 October 2015.